EQUIDISTRIBUTION FOR TORSION POINTS OF A DRINFELD MODULE

DRAGOS GHIOCA

ABSTRACT. We prove an equidistribution result for torsion points of Drinfeld modules of generic characteristic. We also show that similar equidistribution statements provide proofs for the Manin-Mumford and the Bogomolov conjectures for Drinfeld modules.

1. INTRODUCTION

Ullmo proved in [9] the Bogomolov Conjecture for curves embedded in their jacobians and Zhang proved in [10] the Bogomolov Conjecture in full generality. In their proofs they obtain an equidistribution result for points of small height on an abelian variety. Bilu proves in [1] a similar equidistribution statement for points of small height on a power of an algebraic torus. If we restrict our attention only to torsion points of an abelian variety or of a power of the multiplicative group, the above mentioned equidistribution results provide a proof for the Manin-Mumford Conjecture for abelian varieties and, respectively, for powers of the multiplicative group.

Using the analogy between abelian varieties and Drinfeld modules we can ask most of the questions we have for abelian varieties, also in the context of Drinfeld modules (see [8] for a proof of the Manin-Mumford Conjecture for Drinfeld modules of generic characteristic and see [5] for Mordell-Lang statements for Drinfeld modules of both finite and generic characteristic). Denis formulated in [3] the Manin-Mumford and the Mordell-Lang conjectures for Drinfeld modules of generic characteristic. As mentioned above, Denis questions were answered in full in the case of the Manin-Mumford problem (see [8]) and partially in the case of the Mordell-Lang problem (see [5]). We will formulate in Section 4 the Bogomolov Conjecture for Drinfeld modules (see Conjecture 4.9). Similarly, we can ask if the equidistribution results of Bilu, Ullmo and Zhang are valid also in the context of Drinfeld modules. In the present paper we prove an equidistribution result for torsion points of Drinfeld modules of generic characteristic (see Theorem 2.5). We will prove in Section 4 that possible extensions of our equidistribution result lead to a proof of the Bogomolov Conjecture and to a new proof of the Manin-Mumford Conjecture for Drinfeld modules of generic characteristic.

2. STATEMENT OF OUR MAIN RESULT

We define first the notion of a Drinfeld module.

Let p be a prime and let q be a power of p. Let $A := \mathbb{F}_q[t]$. Let K be a field extension of $\mathbb{F}_q$. We fix a morphism $i : A \to K$. We define the operator τ as the power of the usual Frobenius with the property that for every $x \in K$, $\tau(x) = x^q$. Then we let $K\{\tau\}$ be the ring of polynomials in τ with coefficients from K (the addition is the usual addition, while the multiplication is given by the usual composition of functions).

A Drinfeld module is a morphism $\phi : A \to K\{\tau\}$ for which the coefficient of τ^0 in ϕ_a is $i(a)$ for every $a \in A$, and there exists $a \in A$ such that $\phi_a \neq i(a)\tau^0$. In this case, we also say that ϕ is defined over K. For every field extension $K \subset L$, the Drinfeld module ϕ induces an action on $\mathbb{G}_a(L)$ by $a * x := \phi_a(x)$, for each $a \in A$.

Following the definition from [7], we call ϕ a Drinfeld module of generic characteristic if $\ker(i) = \{0\}$ and we call ϕ a Drinfeld module of finite characteristic if $\ker(i) \neq \{0\}$. In the latter case, we say that the characteristic of ϕ is $\ker(i)$ (which is a prime ideal of A). If $\ker(i) = \{0\}$, then we extend i to an embedding of $\mathrm{Frac}(A) = \mathbb{F}_q(t)$ into K.

We note that our definition of a Drinfeld module is not the most general one as we insist on A being the ring of polynomials in one variable over $\mathbb{F}_q$. In the general case, A is the ring of functions defined on a projective non-singular curve C, regular away from a closed point $\infty \in C$. For our definition of a Drinfeld module, $C = \mathbb{P}^1_{\mathbb{F}_q}$ and ∞ is the usual point at infinity on $\mathbb{P}^1$. Before stating our result, we need to introduce several technical ingredients.

Definition 2.1. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module. We call the modular transcendence degree of ϕ the smallest integer $d \geq 0$ such that a Drinfeld module isomorphic to ϕ is defined over a field of transcendence degree d over $\mathbb{F}_q$.

For the remaining of this section, unless otherwise stated, $\phi : A \to K\{\tau\}$ is a Drinfeld module of generic characteristic.

Let v_∞ be the valuation on $F := \mathbb{F}_q(t)$ given by the negative of the degree of any nonzero rational function, i.e.

$$v_\infty\left(\frac{f}{g}\right) = \deg(g) - \deg(f) \text{ for every nonzero } f, g \in \mathbb{F}_q(t).$$

We fix an extension of v_∞ on K (we recall that $F \subset K$, as ϕ is a Drinfeld module of generic characteristic) and we denote it also by v_∞. We let K_∞ be the completion of K at v_∞. We denote by F_∞ the completion of F inside K_∞. We fix an algebraic closure K_∞^{alg} of K_∞ and extend v_∞ to a valuation on K_∞^{alg}. Finally, we let $\mathbb{C}_\infty$ be the completion of K_∞^{alg} at v_∞. As shown in [7], $\mathbb{C}_\infty$ is an algebraically closed, complete valued field. We let K^{alg} and K^{sep} be the algebraic and respectively, the separable closure of K inside K_∞^{alg}.

We define the set $\mathrm{End}_{K^{\mathrm{sep}}}(\phi)$ of endomorphisms of ϕ as the set of all $f \in K^{\mathrm{sep}}\{\tau\}$ such that $f\phi_a = \phi_a f$, for every $a \in A$. As shown in [7], there exists a finite separable extension L of K such that each endomorphism $f \in K^{\mathrm{alg}}\{\tau\}$ of ϕ has coefficients in L. Moreover, $\mathrm{End}_{K^{\mathrm{sep}}}(\phi)$ is a finite extension of A (if we identify $a \in A$ with $\phi_a \in K\{\tau\}$).

We define the torsion submodule of ϕ as

$$\phi_{\mathrm{tor}} = \{x \in K^{\mathrm{alg}} \mid \text{ there exists } a \in A \setminus \{0\} \text{ such that } \phi_a(x) = 0\}.$$

For each nonzero $a \in A$, we let $\phi[a] = \{x \in K^{\mathrm{alg}} \mid \phi_a(x) = 0\}$. Because $A = \mathbb{F}_q[t]$ is a PID, for each $x \in \phi_{\mathrm{tor}}$ there exists a unique monic polynomial $a \in A$ such that $\phi_a(x) = 0$ and for every other $a' \in A$ such that $\phi_{a'}(x) = 0$, then $a|a'$. We call a the *order* of x. Note that by construction, the order of a torsion point is always a monic polynomial in t. Also, we will always identify the greatest common divisor in A of a number of polynomials by the monic generator of the principal ideal of A generated by them. Finally, we note that because ϕ is a Drinfeld module of generic characteristic, $\phi_{\mathrm{tor}} \subset K^{\mathrm{sep}}$.

As shown by Theorem 4.6.9 of [7], there exists an A-lattice $\Lambda \subset \mathbb{C}_\infty$ associated to ϕ (because ϕ has generic characteristic). Let e_ϕ be the exponential function defined in 4.2.3 of

[7] which gives a continuous (in the v_∞-adic topology) isomomorphism

$$\mathrm{e}_\phi : \mathbb{C}_\infty / \Lambda \to \mathbb{C}_\infty .$$

The torsion submodule of ϕ in $\mathbb{C}_\infty$ is isomorphic naturally through e_ϕ^{-1} to $(F \otimes_A \Lambda) / \Lambda$. We let T be the closure of $\phi_{\mathrm{tor}} \subset \mathbb{C}_\infty$ in the v_∞-adic topology of $\mathbb{C}_\infty$. Then the restriction of e_ϕ on $(F_\infty \otimes_A \Lambda) / \Lambda$ gives an isomorphism between $(F_\infty \otimes_A \Lambda) / \Lambda$ and T.

Let r be the rank of Λ and fix an A-basis $z_1, \ldots, z_r$ of Λ. Then $(F \otimes_A \Lambda) / \Lambda \simeq (F/A)^r$. Also, because $F = \mathbb{F}_q(t)$, then $F_\infty = \mathbb{F}_q((\frac{1}{t}))$. Using Proposition 4.6.3 of [7], $(F_\infty \otimes_A \Lambda) / \Lambda$ is isomorphic to $\left(\mathbb{F}_q((\frac{1}{t})) / \mathbb{F}_q[t] \right)^r$. Then we have the isomorphism $\mathrm{E}_\phi : \left(\mathbb{F}_q \left((\frac{1}{t}) \right) / \mathbb{F}_q[t] \right)^r \to T$ given by

$$\mathrm{E}_\phi(\gamma_1, \ldots, \gamma_r) := \mathrm{e}_\phi(\gamma_1 z_1 + \cdots + \gamma_r z_r),$$

for each $\gamma_1, \ldots, \gamma_r \in \mathbb{F}_q \left((\frac{1}{t}) \right) / \mathbb{F}_q[t]$.

We construct the following group isomorphism

$$\sigma : \mathbb{F}_q \left(\left(\frac{1}{t} \right) \right) / \mathbb{F}_q[t] \to \frac{1}{t} \cdot \mathbb{F}_q[[\frac{1}{t}]], \text{ given by}$$

$$(1) \qquad \sigma \left(\sum_{i \geq -n} \alpha_i \left(\frac{1}{t} \right)^i \right) = \sum_{i \geq 1} \alpha_i \left(\frac{1}{t} \right)^i ,$$

for every natural number n and for every $\sum_{i \geq -n} \alpha_i \left(\frac{1}{t} \right)^i \in \mathbb{F}_q \left((\frac{1}{t}) \right)$ (obviously, σ vanishes on $\mathbb{F}_q[t]$). The group $\frac{1}{t} \cdot \mathbb{F}_q[[\frac{1}{t}]]$ is a topological group with respect to the restriction of v_∞ on $\frac{1}{t} \cdot \mathbb{F}_q[[\frac{1}{t}]]$. Hence, the isomorphism σ^{-1} induces a topological group structure on $\mathbb{F}_q \left((\frac{1}{t}) \right) / \mathbb{F}_q[t]$. Therefore, σ becomes a continuous isomorphism of topological groups. We endow $\left(\mathbb{F}_q \left((\frac{1}{t}) \right) / \mathbb{F}_q[t] \right)^r$ with the corresponding product topology. The isomorphism σ extends diagonally to another continuous isomorphism, which we still call σ, between $\left(\mathbb{F}_q((\frac{1}{t})) / \mathbb{F}_q[t] \right)^r$ and $G := \left(\frac{1}{t} \mathbb{F}_q[[\frac{1}{t}]] \right)^r$. Using that e_ϕ is a continuous morphism and using the definition of our topology on $\left(\mathbb{F}_q \left((\frac{1}{t}) \right) / \mathbb{F}_q[t] \right)^r$, we conclude E_ϕ is a continuous morphism. Thus

$$(2) \qquad \mathrm{E}_\phi \, \sigma^{-1} : G \to T \text{ is a continuous isomorphism.}$$

Let μ be the Haar measure on G, normalized so that its total mass is 1. Let $\nu := (\mathrm{E}_\phi \, \sigma^{-1})_* \, \mu$ be the induced measure on T (i.e. $\nu(V) := \mu \left(\sigma \, \mathrm{E}_\phi^{-1}(V) \right)$ for every measurable $V \subset T$). Because μ is a probability measure then ν is also a probability measure. Because μ is a Haar measure on G and $\mathrm{E}_\phi \, \sigma^{-1}$ is a group ismorphism, then ν is a Haar measure on T.

Definition 2.2. For each $x \in K^{\mathrm{sep}}$, we denote by $O(x)$ the (finite) orbit of x under $\mathrm{Gal}(K^{\mathrm{sep}}/\mathrm{K})$.

Definition 2.3. Given $x \in K^{\mathrm{sep}}$, we define a probability measure $\overline{\delta}_x$ on $\mathbb{C}_\infty$ by

$$\overline{\delta}_x = \frac{1}{\#O(x)} \sum_{y \in O(x)} \delta_y,$$

where $\#O(x)$ represents, as always, the cardinality of the set $O(x)$ and δ_y is the Dirac measure on $\mathbb{C}_\infty$ supported on $\{y\}$.

Before we can state the equidistribution result (Theorem 2.5), we need to define the concept of weak convergence for a sequence of probability measures on a metric space.

Definition 2.4. A sequence $\{\lambda_k\}$ of probability measures on a metric space S weakly converge to λ if for any bounded continuous function $f : S \to \mathbb{R}$, $(f, \lambda_k) \to (f, \lambda)$ as $k \to \infty$ (where (f, λ) represents, as always, the integral of f on S with respect to λ). In this case we use the notation $\lambda_k \xrightarrow{w} \lambda$.

Theorem 2.5. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of generic characteristic and of modular transcendence degree at least 2. Assume $\mathrm{End}_{K^{sep}}(\phi) = A$. Let $\{x_k\}$ be a sequence of distinct torsion points in ϕ. Then $\overline{\delta}_{x_k} \xrightarrow{w} \nu$.*

Remark 2.6. If $x \in \phi_{\mathrm{tor}}$, then $O(x) \subset T$ and so, the measure $\overline{\delta}_x$ is supported on T. Therefore, the conclusion of Theorem 2.5 should be interpreted as follows: for each x_k as in Theorem 2.5, $\overline{\delta}_{x_k}$ is a measure on T and as $k \to \infty$, the probability measures $\overline{\delta}_{x_k}$ converge weakly to the normalized Haar measure ν on T.

Remark 2.7. We will explain during the proof of Theorem 2.5 why the hypothesis on the modular transcendence degree is needed in our proof. However, we note that the modular transcendence degree of a Drinfeld module ϕ of generic characteristic is at least 1, because no Drinfeld module isomorphic to ϕ is defined over a finite field (in that case, the Drinfeld module would be of finite characteristic).

3. Proof of the main theorem

We continue in this section with the notation from Section 2.

Proof of Theorem 2.5. Let $\hat{A} := \prod_P A_{(P)}$ denote the profinite completion of A (where P runs over all the monic irreducible polynomials of $A = \mathbb{F}_q[t]$ and $A_{(P)}$ represents the completion of A at the prime ideal (P)). We define the finite adèles $\mathbb{A}_F^f := F \otimes_A \hat{A}$. We let

$$\pi : \mathrm{Gal}(K^{sep}/K) \to \mathrm{GL}_r\left(\mathbb{A}_F^f\right)$$

be the natural representation on the adèlic Tate module of ϕ. Let Γ be its image. The following result is Theorem 3 of [2].

Theorem 3.1. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of generic characteristic. Suppose that $\mathrm{End}_{K^{sep}}(\phi) = A$ and that ϕ is not isomorphic to a Drinfeld module defined over a finite extension of F. Then Γ is an open subgroup of $\mathrm{GL}_r\left(\mathbb{A}_F^f\right)$.*

Remark 3.2. Because we will use Theorem 3.1 in our proof we needed to impose the two extra hypothesis on ϕ: that it has modular transcendence degree at least 2 and its endomorphism ring equals A. As remarked by Pink in a *Note* after the proof of his Theorem 3 in [2], the statement of Theorem 3.1 is conjectured to be true without the extra assumption on the modular transcendence degree. In that case, our proof of Theorem 2.5 would show the equidistribution result for every Drinfeld module of generic characteristic.

Because our Drinfeld module ϕ has modular transcendence degree at least 2, it is not isomorphic to a Drinfeld module defined over a finite extension of F (otherwise, it would have modular transcendence degree 1; see also Remark 2.7). Thus ϕ satisfies the hypothesis of Theorem 3.1 and so, Γ is an open subgroup of $\mathrm{GL}_r\left(\mathbb{A}_F^f\right)$. Hence

$$(3) \qquad\qquad [\mathrm{GL}_r\left(\mathbb{A}_F^f\right) : \Gamma] < \aleph_0.$$

Using (3) we conclude there exist finitely many irreducible monic polynomials $P_1, \ldots, P_l \in A$ and there exists a natural number m such that

$$\text{(4)} \qquad \prod_{i=1}^{l} \left(I_r + \left(\prod_{i=1}^{l} P_i \right)^m \text{GL}_r \left(A_{(P_i)} \right) \right) \cdot \prod_{P \neq P_i} \text{GL}_r \left(A_{(P)} \right) \subset \Gamma,$$

where $I_r \in \text{GL}_r$ is the identity matrix. Therefore, (4) shows that the orbit of every torsion point of ϕ of order a (where $a \in A$ is a monic polynomial) coprime with $\prod_{i=1}^{l} P_i$ consists of all the possible torsion points of order a.

In general, we represent a torsion point x of order b (not necessarily coprime with $P_1 \ldots P_l$) through the isomorphism $\sigma \, \text{E}_\phi^{-1} : \phi_{\text{tor}} \to \left(\frac{1}{t} \mathbb{F}_q[[\frac{1}{t}]] \right)^r$, as

$$\text{(5)} \qquad \left(\frac{b_1}{b}, \ldots, \frac{b_r}{b} \right)$$

where

(6)   each polynomial b_i has degree less than b

and, moreover, the greatest common divisor

$$\text{(7)} \qquad (b_1, \ldots, b_r, b) = 1.$$

Then the orbit $O(x)$ of x corresponds through $\sigma \, \text{E}_\phi^{-1}$ to a subset $S(x)$ of the set of all possible tuples in $G = \left(\frac{1}{t} \mathbb{F}_q[[\frac{1}{t}]] \right)^r$ of the form (5) satisfying (6) and (7). Let $H \subset \text{Gal}(K^{\text{sep}}/K)$ be the preimage through π^{-1} of the subgroup from (4) which is contained in Γ. Then $\text{Gal}(K^{\text{sep}}/K)$ is a finite union of cosets of H.

For each $i \in \{1, \ldots, l\}$, let β_i the exponent of P_i in the prime decomposition of b. Let $b' := \prod_{i=1}^{l} P_i^{\beta_i'}$ be the monic polynomial which is the greatest common divisor between b and $P := \left(\prod_{i=1}^{l} P_i \right)^m$. Obviously, $\beta_i' \leq \beta_i$. For each $i \in \{1, \ldots, l\}$, let

$$\text{(8)} \qquad \left(\frac{\alpha_1}{P_i^{\beta_i}}, \ldots, \frac{\alpha_r}{P_i^{\beta_i}} \right)$$

be the image in $S(x)$ of an element of the P_i-power part of $O(x)$. Then (4) shows that the image through H of the P_i-power part of the torsion point from (8) corresponds in $S(x)$ to all the elements of the form

$$\text{(9)} \qquad \left(\frac{\alpha_1 + P_i^{\beta_i'} q_1}{P_i^{\beta_i}}, \ldots, \frac{\alpha_r + P_i^{\beta_i'} q_r}{P_i^{\beta_i}} \right)$$

for arbitrary $q_1, \ldots, q_r$.

For a monic, prime polynomial $Q \in A$, different than $P_1, \ldots, P_l$, let Q^β be the maximal power of Q dividing b. Then, by (4), the Q-power part of the orbit $O(x)$ consists of all torsion points of ϕ of order Q^β.

Let $\{x_k\}$ be a sequence of distinct torsion points of ϕ. Because ϕ has generic characteristic, then $\{x_k\} \subset K^{\text{sep}}$. Because the elements of the sequence $\{x_k\}$ are distinct, the orders $b_k \in A = \mathbb{F}_q[t]$ of each x_k have the property that $\deg(b_k) \to \infty$ (the degree $\deg(b_k)$ of each b_k is the degree of b_k as a polynomial in t).

For each k we let $O_k := \sigma \, \mathrm{E}_\phi^{-1}(O(x_k)) \subset G$. For each k we define by $\overline{\delta}_k$ the associated probability measure on G, equally supported on O_k:

$$\overline{\delta}_k := \frac{1}{\#O_k} \sum_{y \in O_k} \delta_y.$$

Because $\mathrm{E}_\phi \, \sigma^{-1} : G \to T$ is a continuous isomorphism, we conclude that it suffices to show

(10)
$$\overline{\delta}_k \xrightarrow{w} \mu.$$

Let f be any continuous, real valued function on G. Because G is a totally disconnected, compact space, f is a finite $\mathbb{R}$-linear combination of characteristic functions on open subsets of G. Hence, in order to prove (10), it suffices to prove (10) for characteristic functions of open subsets of G. Thus, for each such open subset U, we need to show

(11)
$$\frac{\#(O_k \cap U)}{\#O_k} \to \mu(U) \text{ as } k \to \infty.$$

Let U be an open subset of G. Then U is of the form

$$\left(a_1\left(\frac{1}{t}\right), \ldots, a_r\left(\frac{1}{t}\right) \right) + \left(\frac{1}{t^{n_1+1}} \mathbb{F}_q\left[\left[\frac{1}{t}\right]\right], \ldots, \frac{1}{t^{n_r+1}} \mathbb{F}_q\left[\left[\frac{1}{t}\right]\right] \right),$$

where $a_i \in \frac{1}{t}\mathbb{F}_q[\frac{1}{t}]$ is a polynomial of degree at most n_i for each i, and $n_1, \ldots, n_r$ are positive integers. Ultimately, our goal is to show

(12)
$$\frac{\#(O_k \cap U)}{\#O_k} \to \mu(U) = q^{-\sum_{i=1}^{r} n_i}, \text{ as } k \to \infty.$$

Let O be one of the sets O_k. Let $b \in \mathbb{F}_q[t]$ be the monic polynomial which is the order of x_k. Then all the torsion points $y \in O(x_k)$ have the same order b. Therefore, the elements of O are of the form

(13)
$$\left(\frac{b_1}{b}, \ldots, \frac{b_r}{b} \right),$$

where $b_i \in \mathbb{F}_q[t]$ and for each i,

(14)
$$\deg(b_i) < \deg(b)$$

and moreover, the greatest common divisor

(15)
$$(b_1, \ldots, b_r, b) = 1.$$

Theorem 3.1 will allow us to determine the proportion of elements of the form (13) which are in O. This will allow us to compute $\#(O \cap U)$, which in turn will lead to the proof of our Theorem 2.5.

Let b' be the greatest common divisor of b and $\prod_{i=1}^{l} P_i^m$. We let C be the collection of all tuples of polynomials of the form

(16)
$$(\alpha_1, \ldots, \alpha_r) \text{ with } \deg(\alpha_i) < \deg(b') \text{ for all } i$$

such that for each such tuple there exists $y \in O$ of the form

(17)
$$\left(\frac{\alpha_1 + b'q_1}{b}, \ldots, \frac{\alpha_r + b'q_r}{b} \right),$$

6

where for each i, $q_i \in \mathbb{F}_q[t]$ and

(18)
$$\deg(\alpha_i + b'q_i) < \deg(b)$$

and

(19)
$$(\alpha_1 + b'q_1, \ldots, \alpha_r + b'q_r, b) = 1.$$

If $b' = 1$, then the only tuple as in (16) is $(\alpha_1, \ldots, \alpha_r) = (0, \ldots, 0)$.

Condition (19) shows that

(20)
$$(\alpha_1, \ldots, \alpha_r, b') = 1.$$

Clearly, C is a finite set because there are finitely many tuples of the form (16) without even asking the extra condition (17). Using (4) and our analysis for the action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on the different Q-power parts of O, we conclude that the elements of O are *all* the elements of G of the form (17), corresponding to some tuple $(\alpha_1, \ldots, \alpha_r) \in C$, and satisfying the conditions (18) and (19).

We fix a tuple $(\alpha_1, \ldots, \alpha_r) \in C$. We count the number of elements of O which are of the form (17) for this tuple $(\alpha_1, \ldots, \alpha_r)$. As explained above, because of (4) we need to count the number of all elements G of the form (17), corresponding to this fixed tuple $(\alpha_1, \ldots, \alpha_r)$, and satisfying (18) and (19).

We define the Möbius function μ on the set of all monic polynomials in $\mathbb{F}_q[t]$ by

$$\mu(1) = 1,$$

$$\mu(Q_1 Q_2 \ldots Q_n) = (-1)^n \text{ if } Q_1, \ldots, Q_n \text{ are distinct irreducible, non-constant polynomials,}$$

$$\mu(f) = 0 \text{ if } f \text{ is not squarefree.}$$

In this proof, the letter μ also appears as denoting the measure on G. This should not be confused with the above defined Möbius function, as the measure μ is always evaluated on subsets of G, while the Möbius function μ is always evaluated on monic polynomials.

It is immediate to see that for every nonzero polynomial $f \in \mathbb{F}_q[t]$ (monic or not)

(21)
$$\sum_{g|f} \mu(g) = 1 \text{ if } \deg(f) = 0 \text{ and it is } 0 \text{ otherwise.}$$

Of course, g in (21) is a monic polynomials and in general, when we will sum over divisors of a polynomial f, we will always include only the monic polynomials dividing f.

Hence, in order to count the number of elements of O which are of the form (17) for the fixed tuple $(\alpha_1, \ldots, \alpha_r)$, we compute

(22)
$$\sum_{\substack{q_1, \ldots, q_r \\ \deg(\alpha_1 + b'q_1) < \deg(b), \ldots, \deg(\alpha_r + b'q_r) < \deg(b)}} \left(\sum_{d | (\alpha_1 + b'q_1, \ldots, \alpha_r + b'q_r, b)} \mu(d) \right).$$

Using (21), we obtain that the inner sum in (22) equals 1 if and only if the greatest common divisor $(\alpha_1 + b'q_1, \ldots, \alpha_r + b'q_r, b) = 1$, otherwise the inner sum equals 0. Changing the order

of summation in (22) we obtain

$$(23) \qquad \sum_{d|b} \mu(d) \cdot \left(\sum_{\substack{q_1,\ldots,q_r \\ \deg(\alpha_1+b'q_1)<\deg(b),\ldots,\deg(\alpha_r+b'q_r)<\deg(b) \\ d|(\alpha_1+b'q_1),\ldots,d|(\alpha_r+b'q_r)}} 1 \right).$$

We evaluate the inner sum taken into account that for its computation, $\alpha_1, \ldots, \alpha_r$ and b, b' and d are all fixed. We also take into account that if d and b' are not coprime, then the inner sum is 0 as shown by (20). On the other hand, if d and b' are coprime, then each congruence

(24) $\qquad \alpha_i + b'q_i \equiv 0 \pmod{d}$ has one incongruent solution q_i modulo d.

For each i, let s_i be the unique solution to the congruence (24) with $\deg(s_i) < \deg(d)$. Then all the solutions q_i to the congruence (24), which we count in the inner sum from (23), are of the form

$$(25) \qquad q_i = s_i + dq_i',$$

for some polynomials q_i' such that

$$(26) \qquad \deg(\alpha_i + b'q_i) < \deg(b).$$

Using (25) we get

$$(27) \qquad \alpha_i + b'q_i = \alpha_i + b's_i + b'dq_i'.$$

Because the inner sum of (23) is nonzero only if $(d, b') = 1$ and because $d|b$, we need to estimate the inner sum of (23) only when $d | \frac{b}{b'}$ (and even then, the inner sum still might be 0). So, for us, $\deg(d) \leq \deg(b) - \deg(b')$. This shows

$$\deg(\alpha_i + b's_i) \leq \max\{\deg(\alpha_i), \deg(b') + \deg(s_i)\} < \max\{\deg(b'), \deg(b') + \deg(d)\} \leq \deg(b).$$

Therefore, for each i and for each polynomial q_i' of degree less than $\deg(b) - \deg(b'd)$, the degree of (27) is less than the degree of b. Hence, we have $q^{(\deg(b)-\deg(b'd))r}$ choices for tuples $(q_1', \ldots, q_r')$. So, we compute the inner sum in (23) and obtain

$$(28) \qquad q^{r(\deg(b)-\deg(b'd))} = q^{r(\deg(b)-\deg(b'))-r\deg(d)},$$

if $(d, b') = 1$, while if $(d, b') \neq 1$, the inner sum in (23) is 0. We use (28) in (23) and obtain

$$(29) \qquad \sum_{\substack{d|b \\ (d,b')=1}} \mu(d)q^{r(\deg(b)-\deg(b'))-r\deg(d)} = q^{r(\deg(b)-\deg(b'))} \sum_{\substack{d|b \\ (d,b')=1}} \mu(d)q^{-r\deg(d)}.$$

We observe that the result we obtained in (29) is independent of the particular choice of the tuple $(\alpha_1, \ldots, \alpha_r)$. Now we compute, for the same fixed tuple $(\alpha_1, \ldots, \alpha_r)$, the number of elements of O of the form (17) which are also in U. As explained before, using (4), we need to count the number of all elements of U of the form (17), corresponding to this fixed tuple $(\alpha_1, \ldots, \alpha_r)$, and satisfying (18) and (19).

For each $i \in \{1, \ldots, r\}$, we let $a_i'(t) := t^{n_i} a_i(\frac{1}{t})$, where $a_i'(t)$ is a polynomial of degree less than n_i (we are using the fact that $a_i(\frac{1}{t}) \in \frac{1}{t}\mathbb{F}_q[\frac{1}{t}]$ is a polynomial of degree n_i). The

8

requirement for an element of O of the form (17) to lie in U is given by

$$(30) \qquad v_\infty\left(\frac{\alpha_i + b'q_i}{b} - \frac{a'_i}{t^{n_i}}\right) \geq n_i + 1 \text{ for each } i.$$

Inequality (30) is equivalent with

$$(31) \qquad \deg\left(t^{n_i}(\alpha_i + b'q_i) - ba'_i\right) \leq \deg(b) - 1.$$

Thus when we count the number of elements of $O \cap U$ which are of the form (17) for one fixed tuple $(\alpha_1, \ldots, \alpha_r) \in C$, we obtain the same sum as in (22), only that now we have the extra assumption (31) on top of the other restrictions on q_i. Again we can change the order of summation in (22) and obtain (23), only that the inner summation is over all q_i which also satisfy (31). We obtain once again (25) and we use it in (31) to get

$$(32) \qquad \deg\left(t^{n_i}(\alpha_i + b's_i + b'dq'_i) - ba'_i\right) \leq \deg(b) - 1.$$

We are interested in estimating $\#(O \cap U)$ when $\deg(b)$ is much larger than the degree of b' (and implicitly, much larger than the degrees of the α_i, as $\deg(\alpha_i) < \deg(b')$) and also much larger than the numbers n_i. This is the case because our goal is to prove (11), and as $k \to \infty$, $\deg(b) \to \infty$, while U is fixed. Note that the degree of b' is bounded by the degree of $P = \prod_{i=1}^l P_i^m$ (which is a fixed polynomial) and the numbers n_i are fixed the moment we fixed U, while b is the order of one of the elements of our infinite sequence of distinct torsion points.

We go back now to (31). We know that $\deg(q_i) < \deg(b) - \deg(b')$ (see (18)). Thus, using (25), we get $\deg(q'_i) < \deg(b) - \deg(b') - \deg(d)$. Therefore, let

$$q'_i = \sum_{j=0}^{\deg(b)-\deg(b')-\deg(d)-1} \gamma_j^{(i)} t^j,$$

where some of the $\gamma_j^{(i)} \in \mathbb{F}_q$ could be 0 (including some of the top coefficients).

Let L be the degree of P and let $n_0 := \max\{n_1, \ldots, n_r\} + 1$. Assume for the moment that

$$(33) \qquad \deg(d) \leq \deg(b) - L - n_0 < \deg(b) - \deg(b') - n_i,$$

where in the second inequality from (33) we also used the fact that $b' | P$ (and so, $\deg(b') \leq \deg(P)$). Under our assumption (33), we obtain that the top n_i coefficients $\gamma_j^{(i)}$ of q'_i are determined by the coefficients of d, b', b, α_i and a'_i and by condition (32), while the remaining $(\deg(b) - \deg(b') - \deg(d) - n_i)$ coefficients $\gamma_j^{(i)}$ can be arbitrary elements of $\mathbb{F}_q$. Hence, under the assumption (33), we obtain that the inner sum in (23) associated only to the elements in U of the form (17) equals

$$(34) \qquad q^{\sum_{i=1}^r (\deg(b)-\deg(b')-\deg(d)-n_i)},$$

if $(b', d) = 1$, while if $(b', d) > 1$, the inner sum in (23) is 0.

Next we analyze the case $\deg(d) > \deg(b) - L - n_0$. In this case, (32) shows that $\deg(q'_i) < L + n_0$. Thus, the inner sum in (23) can contribute at most $q^{r(L+n_0)}$ and this computation is without even taking into consideration the actual restrictions on the coefficients imposed by (32).

Combining our findings in both cases with respect to assumption (33), we conclude that the number of elements in $O \cap U$ which are of the form (17) for a fixed $(\alpha_1, \ldots, \alpha_r) \in C$ is

$$(35) \qquad \sum_{\substack{d|b \\ (d,b')=1 \\ \deg(d) \le \deg(b)-L-n_0}} \mu(d)q^{r(deg(b)-\deg(b')-\deg(d))-\sum_{i=1}^r n_i} + \sum_{\substack{d|b \\ (d,b')=1 \\ \deg(d)>\deg(b)-L-n_0}} O(q^{r(L+n_0)}),$$

where the O-notation in the above second sum is the classical one and it refers in our context to the fact that the summand in the second sum from (35) is at most $q^{r(L+n_0)}$ regardless of b. We note that the O-notation has nothing to do with our notation for orbits or for the set O, as the O-notation will always have attached to it, in parenthesis, a certain real number.

Because of the degree condition for d in the second sum in (35), we know there are at most q^{L+n_0} possibilities for d (for each fixed b), because $\deg\left(\frac{b}{d}\right) < L + n_0$. Hence, the second sum from (35) is of the order of $q^{(r+1)(L+n_0)}$. Introducing this estimate in (35) and adding and subtracting from (35) the quantity

$$\sum_{\substack{d|b \\ (d,b')=1 \\ \deg(d)>\deg(b)-L-n_0}} \mu(d)q^{r(deg(b)-\deg(b')-\deg(d))-\sum_{i=1}^r n_i},$$

we obtain the following estimate for (35):

$$(36)$$
$$\sum_{\substack{d|b \\ (d,b')=1}} \mu(d)q^{r(deg(b)-\deg(b'd))-\sum_{i=1}^r n_i} - \sum_{\substack{d|b \\ (d,b')=1 \\ \deg(d)>\deg(b)-L-n_0}} \mu(d)q^{r(deg(b)-\deg(b'd))-\sum_{i=1}^r n_i} + O(1).$$

Note that in the O-estimate from (36), we replaced $O\left(q^{(r+1)(L+n_0)}\right)$ by $O(1)$, because q, r and L are always fixed, while n_0 is fixed the moment we fix U.

We estimate the second sum in (36) and we easily conclude it is also $O\left(q^{(r+1)(L+n_0)}\right)$. Hence the sum in (36) is

$$(37) \qquad q^{r(\deg(b)-\deg(b'))-\sum_{i=1}^r n_i} \sum_{\substack{d|b \\ (d,b')=1}} \mu(d)q^{-r \deg(d)} + O\left(q^{(r+1)(L+n_0)}\right).$$

The sum in (37) is the number of elements in $O \cap U$ of the form (17) for a fixed $(\alpha_1, \ldots, \alpha_r)$. Note that r, L, n_0 are all constant as $\deg(b) \to \infty$. As explained before, the number of tuples $(\alpha_1, \ldots, \alpha_r) \in C$ depends on x_k (we recall that O and b were associated to some torsion element x_k from our infinite sequence), but the cardinality of C has the fixed upper bound q^{Lr} because $b'|P$ and $\deg(P) = L$ and all of the polynomials α_i have degree less than $\deg(b')$ for each i. So, in order to prove (12), we use (29) and (37) and we are done if we show

$$(38) \qquad q^{r(\deg(b)-\deg(b'))} \sum_{\substack{d|b \\ (d,b')=1}} \mu(d)q^{-r \deg(d)} \to \infty$$

as $\deg(b) \to \infty$. Let b_0 be the product of all the powers of irreducible polynomials dividing b other than the powers of the polynomials $P_1, \ldots, P_l$. Thus b_0 is the largest divisor of b

coprime with b'. Then the sum in (38) can be rewritten as

$$(39) \qquad \sum_{d|b_0} \mu(d) q^{-r \deg(d)}.$$

The sum in (39) equals

$$(40) \qquad \prod_{\substack{c \text{ irreducible} \\ c|b_0}} \left(1 - \frac{1}{q^{r \deg(c)}}\right).$$

We observe that all the factors in the product (40) are less than 1 and so, if we extend the product (40) to include also the possible prime divisors of b from the set $\{P_1, \ldots, P_l\}$, we can only decrease our product. So, to prove (38), it suffices to show

$$(41) \qquad q^{r(\deg(b) - \deg(b'))} \prod_{\substack{c \text{ irreducible} \\ c|b}} \left(1 - \frac{1}{q^{r \deg(c)}}\right) \to \infty$$

as $\deg(b) \to \infty$. We note that $\deg(b') \leq L$ (as it was remarked previously in our proof, because $b'|P$ and $\deg(P) \leq L$). So, we only need to show

$$(42) \qquad q^{r \deg(b)} \prod_{\substack{c \text{ irreducible} \\ c|b}} \left(1 - \frac{1}{q^{r \deg(c)}}\right) \to \infty \text{ as } \deg(b) \to \infty.$$

Consider the prime factorization of $b = \prod_{i=1}^{s} c_i^{e_i}$ in monic polynomials. Then the left hand side of (42) reads

$$(43) \qquad \prod_{i=1}^{s} q^{r(e_i - 1) \deg(c_i)} \left(q^{r \deg(c_i)} - 1\right).$$

Because ϕ has modular transcendence degree at least 2, the rank r of ϕ is at least 2 (otherwise, ϕ_t is a polynomial of degree q, which means that ϕ is isomorphic over K^{alg} with a Drinfeld module ψ for which $\psi_t = t\tau^0 + \tau$; hence ϕ would be isomorphic with a Drinfeld module defined over F). Because $r \geq 2$, we obtain $q^{r \deg(c_i)} - 1 \geq q^{\frac{r \deg(c_i)}{2}}$ for each i.

As $\deg(b) \to \infty$, then $\sum_{i=1}^{s} e_i \deg(c_i) \to \infty$, which proves

$$(44) \qquad \prod_{i=1}^{s} q^{r(e_i - 1) \deg(c_i)} \left(q^{r \deg(c_i)} - 1\right) \geq q^{\frac{r \sum_{i=1}^{s} e_i \deg(c_i)}{2}} \to \infty.$$

This concludes the proof of (11), which proves Theorem 2.5. $\qquad \square$

Remark 3.3. Note that even if we used also in the last part of our argument the fact that $r \geq 2$, the only place where we used crucially the fact that ϕ has mdular transcendence degree at least 2 was in Pink's result (Theorem 3.1). Therefore, if Pink's result were true for any Drinfeld module of generic characteristic, then our proof of Theorem 2.5 would also hold for any such Drinfeld module. The limit in (42) is infinite even if $r = 1$ (in which case ϕ would have modular transcendence degree 1).

4. The Bogomolov Conjecture and the Manin-Mumford Theorem for Drinfeld modules

In this section, all subvarieties are *closed* subvarieties.

Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of generic characteristic. For each positive integer g, we let ϕ act on $\mathbb{G}_a^g$ diagonally. Therefore, we may define just as before the torsion points of the action of ϕ on $\mathbb{G}_a^g$ as all the g-tuples $(x_1, \ldots, x_g)$ for which there exists a nonzero $a \in A$ such that $\phi_a(x_i) = 0$ for each i. We believe a similar equidistribution result as our Theorem 2.5 holds for the torsion points of $\mathbb{G}_a^g$. Before stating our conjecture, we require the following definitions.

Definition 4.1. An algebraic ϕ-submodule of $\mathbb{G}_a^g$ is a K^{sep}-algebraic subvariety of $\mathbb{G}_a^g$ which is invariant under the action of ϕ.

Definition 4.2. A torsion subvariety of $\mathbb{G}_a^g$ is a translate of an irreducible algebraic ϕ-submodule of $\mathbb{G}_a^g$ by a torsion point.

Definition 4.3. A sequence of points $\{x_k\} \subset \mathbb{G}_a^g(K^{\mathrm{alg}})$ is strict if any proper torsion subvariety of $\mathbb{G}_a^g$ contains x_k for only finitely many values of k.

For a point $x \in \mathbb{G}_a^g(K^{\mathrm{sep}})$, we let as before $O(x)$ denote the (finite) orbit of x under the diagonal action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on $\mathbb{G}_a^g(K^{\mathrm{sep}})$. We also define the associated probability measure $\overline{\delta}_x$ on $\mathbb{C}_\infty{}^g$ for such an orbit $O(x)$:

$$\overline{\delta}_x := \frac{1}{\#O(x)} \sum_{y \in O(x)} \delta_y.$$

Finally, we denote by $\nu^{(g)}$ the product measure on T^g corresponding to ν taken g times.

Conjecture 4.4. Let ϕ be a Drinfeld module of generic characteristic. Assume $\mathrm{End}_{K^{\mathrm{sep}}}(\phi) = A$. Let $\{x_k\}$ be a strict sequence of torsion points in $\mathbb{G}_a^g(K^{\mathrm{alg}})$, for some $g \geq 1$. Then $\overline{\delta}_{x_k} \xrightarrow{w} \nu^{(g)}$.

Remarks 4.5. We used in Conjecture 4.4 the same convention as explained in Remark 2.6, regarding the measures $\overline{\delta}_{x_k}$. Because their support is contained in T^g, we interpret them as probability measures on T^g, rather than as probability measures on the larger space $\mathbb{C}_\infty{}^g$.

We did not include in our Conjecture 4.4 the hypothesis that ϕ has modular transcendence degree at least 2 (as we did in our Theorem 2.5), because, as mentioned before, it is believed that Pink's Theorem 3.1 holds without this extra hypothesis on ϕ.

We require in our Conjecture 4.4 the hypothesis on the sequence $\{x_k\}$ being strict because otherwise the support of the limit measure would lie on a proper subvariety of T^g. In the case $g = 1$, our hypothesis in Theorem 2.5 that the sequence $\{x_k\} \subset K^{\mathrm{alg}}$ contains distinct torsion points suffices for the condition that the sequence is strict (because the torsion subvarieties of $\mathbb{G}_a$ are the torsion points of ϕ). Actually, our proof of Theorem 2.5 follows precisely the same way under the slightly weaker hypothesis that the sequence $\{x_k\} \subset \phi_{\mathrm{tor}}$ contains each torsion point of ϕ at most finitely many times (this condition being equivalent with the condition that $\{x_k\}$ is strict).

A positive answer to our Conjecture 4.4 would provide a proof to the following result (the Manin-Mumford Theorem for Drinfeld modules of generic characteristic).

Theorem 4.6. *Let* $\phi : A \to K\{\tau\}$ *be a Drinfeld module of generic characteristic. Assume* $\mathrm{End}_{K^{\mathrm{sep}}}(\phi) = A$. *Let* $g \geq 1$ *and let* X *be an irreducible* K^{sep}*-subvariety of* $\mathbb{G}_a^g$ *(i.e., an irreducible closed subvariety of the g-dimensional affine space). If* $X(K^{\mathrm{sep}}) \cap \phi_{\mathrm{tor}}^g$ *is Zariski dense in* X, *then* X *is a torsion subvariety of* $\mathbb{G}_a^g$.

As mentioned in Section 1, Theorem 4.6 was proved by Scanlon in [8] using the methods of model theory of difference fields. His result is valid even without the extra assumption that the endomorphism ring of ϕ equals A. However, a positive answer to Conjecture 4.4 would provide a completely different proof of Theorem 4.6, given purely in the language of number theory.

Moreover, we believe that an equidistribution result, similar to the results proved by Bilu, Ullmo and Zhang, holds also for points of small height associated to the action of a Drinfeld module (see [4] or [6] for the definition of the height $\widehat{\mathrm{h}}$ associated to a Drinfeld module).

Conjecture 4.7. *Let* $\phi : A \to K\{\tau\}$ *be a Drinfeld module of generic characteristic and let* $g \geq 1$. *Assume* $\mathrm{End}_{K^{\mathrm{sep}}}(\phi) = A$. *Let* $\{x_k\} \subset \mathbb{G}_a^g(K^{\mathrm{sep}})$ *be a strict sequence. If* $\lim_{k \to \infty} \widehat{\mathrm{h}}(x_k) = 0$, *then* $\overline{\delta}_{x_k} \xrightarrow{w} \nu^{(g)}$.

Remarks 4.8. The measures $\overline{\delta}_{x_k}$ are probability measures on $\mathbb{C}_\infty{}^g$, while $\nu^{(g)}$ is the normalized Haar measure on T^g. Therefore, we interpret the conclusion of Conjecture 4.7 as follows: the measures $\overline{\delta}_{x_k}$ converge weakly to the probability measure $\nu^{(g)}$ on $\mathbb{C}_\infty{}^g$, which is supported on T^g (and the restriction of $\nu^{(g)}$ on T^g is a Haar measure).

Conjecture 4.4 is a particular case of Conjecture 4.7 because all the torsion points of a Drinfeld module have height 0.

An equidistribution result as Conjecture 4.7 would lead to the following form of the Bogomolov Conjecture in the context of Drinfeld modules of generic characteristic.

Conjecture 4.9. *Let* $\phi : A \to K\{\tau\}$ *be a Drinfeld module of generic characteristic. Assume* $\mathrm{End}_{K^{\mathrm{sep}}}(\phi) = A$. *Let* $g \geq 1$ *and let* X *be an irreducible* K^{sep}*-subvariety of* $\mathbb{G}_a^g$. *For each* $n \geq 1$, *we let*

$$X_n := \{x \in X(K^{\mathrm{sep}}) \mid \widehat{\mathrm{h}}(x) < \frac{1}{n}\}.$$

If for each $n \geq 1$, X_n *is Zariski dense in* X, *then* X *is a torsion subvariety of* $\mathbb{G}_a^g$.

We can also formulate the Manin-Mumford and the Bogomolov questions for Drinfeld modules of finite characteristic. However, we cannot always expect the conclusion be that the variety X is a torsion subvariety (see Section 4 of [6] for a comprehensive discussion of the pathologies appearing in finite characteristic Drinfeld modules).

We will show how to deduce Theorem 4.6 and Conjecture 4.9 from Conjecture 4.4 and, respectively Conjecture 4.7. More precisely, we will show that knowing the validity of Conjectures 4.4 and 4.7 for all $g \leq N$ implies the conclusions of Theorem 4.6 and, respectively Conjecture 4.9 for $g = N$. Our proofs are inspired by the arguments from the proof of Theorem 5.1 of [1].

We first need a relative notion of the condition that a sequence is strict.

Definition 4.10. *Let* Y *be an algebraic* ϕ*-submodule of* $\mathbb{G}_a^N$ *and let* $\{x_k\} \in Y(K^{\mathrm{sep}})$ *be a sequence of points in* Y. *We call the sequence* $\{x_k\}$ *strict relative to* Y *if any torsion subvariety of* Y *of dimension smaller than* $\dim(Y)$ *contains* x_k *for only finitely many values of* k.

We will also use the following result.

Lemma 4.11. *Let Y be a subvariety of $\mathbb{G}_a^g$ such that $\phi_t(Y) \subset Y$. Then every irreducible component of Y is a torsion subvariety.*

Proof. Let $Y_1, \ldots, Y_m$ be the irreducible components of Y. Then for each $i \in \{1, \ldots, m\}$ and for each $n \geq 1$, there exists $j(i, n) \in \{1, \ldots, m\}$ such that $\phi_{t^n}(Y_i) = Y_{j(i,n)}$ (because $\phi_{t^n}(Y_i)$ is also an irreducible component of Y). Hence, for each $i \in \{1, \ldots, m\}$, there exist positive integers $n_1 < n_2$ 9depending on i) such that $\phi_{t^{n_1}}(Y_i) = \phi_{t^{n_2}}(Y_i)$. Thus, $\phi_{t^{n_1}}(Y_i)$ is invariant under $\phi_{t^{n_2-n_1}}$. Using Lemme 4 of [3] we conclude $\phi_{t^{n_1}}(Y_i)$ is a torsion subvariety. Therefore, using that Y_i is irreducible, we obtain that also Y_i is a torsion subvariety. $\qquad \square$

The following lemma is a classical result, whose proof we include for completeness.

Lemma 4.12. *Let S be an infinite set in K^{alg} and let $n \geq 1$. Then S^n (the cartesian product of S with itself n times) is Zariski dense in $\mathbb{G}_a^n$.*

Proof. We prove the statement of our lemma by induction on n. For $n = 1$, the statement is clear, as every infinite set is Zariski dense in the 1-dimensional affine space. Next we assume the lemma holds for n and we will prove it for $n + 1$.

Let $f \in K^{\mathrm{alg}}[X_1, \ldots, X_{n+1}]$ be a polynomial vanishing on S^{n+1}. We will prove $f = 0$, which will show that indeed, S^{n+1} is Zariski dense in $\mathbb{G}_a^{n+1}$. For each $\alpha \in S$, $f(X_1, \ldots, X_n, \alpha)$ vanishes on $S^n \subset \mathbb{G}_a^n$. Using the induction hypothesis, we conclude

$$(45) \qquad\qquad f(X_1, \ldots, X_n, \alpha) = 0.$$

We consider $f \in K^{\mathrm{alg}}(X_1, \ldots, X_n)[X_{n+1}]$ as a polynomial of only the variable X_{n+1}. Because (45) holds for the (infinitely many) elements $\alpha \in S$, we conclude $f = 0$, as desired. $\qquad \square$

Because $\phi_{\mathrm{tor}} \subset K^{\mathrm{alg}}$ is infinite, we obtain the following consequence of Lemma 4.12.

Corollary 4.13. *For each $n \geq 1$, the torsion submodule ϕ_{tor}^n is Zariski dense in $\mathbb{G}_a^n$.*

Moreover, the following is also true.

Corollary 4.14. *Let $Y \subset \mathbb{G}_a^N$ be an algebraic ϕ-submodule. Then $\phi_{\mathrm{tor}}^N \cap Y$ is Zariski dense in Y.*

Proof. Let Y_0 be the connected component of Y. Then Y_0 is isomorphic to $\mathbb{G}_a^M$ for $M := \dim(Y)$. Using Corollary 4.13, we conclude $\phi_{\mathrm{tor}}^N \cap Y_0$ is Zariski dense in Y_0. Moreover, because all the irreducible components of Y are translates of Y_0 by torsion points (see Lemma 4.11), we conclude that $\phi_{\mathrm{tor}}^N \cap Y$ is Zariski dense in Y. $\qquad \square$

We first show that the validity of Conjecture 4.4 for all $g \leq N$ yields the following key result.

Theorem 4.15. *Let Y be an algebraic ϕ-submodule of $\mathbb{G}_a^N$ and let X be a K^{sep}-subvariety of Y. Then X has at most finitely many maximal torsion subvarieties.*

Proof of Theorem 4.15. We prove our theorem by induction on $\dim(Y)$. The case $\dim(Y) = 0$ is trivial, as then Y consists of only finitely many torsion points.

Assume Theorem 4.15 holds for $\dim(Y) < M \leq N$ and we will prove it for varieties of dimension M.

First we note that without loss of generality we may assume $\dim(X) < M$. Indeed, if $\dim(X) = M$, then the M-dimensional irreducible components of X are also irreducible components of Y. But the irreducible components of Y are torsion subvarieties by Lemma 4.11. Removing the irreducible components of X which are also irreducible components of Y would make X have strictly smaller dimension than M and would not change the conclusion of Theorem 4.15, because we would remove only finitely many maximal torsion subvarieties of X. Hence, we may assume $\dim(X) < M$.

Secondly, we may replace X with

$$\bigcup_{\sigma \in \mathrm{Gal}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})} \sigma(X)$$

and replace Y with

$$\bigcup_{\sigma \in \mathrm{Gal}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})} \sigma(Y),$$

which remains an algebraic ϕ-module because the action of ϕ is invariant under $\mathrm{Gal}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$. If our Theorem 4.15 would fail for $X \subset Y$ in the first place, then it would also fail for the above varieties which replace them. The advantage of our reduction is that both Y and X are now invariant under $\mathrm{Gal}(\mathrm{K}^{\mathrm{sep}}/\mathrm{K})$. Note that while making this reduction we do not change the dimension of X. So, we still have $\dim(X) < M$.

Assume X has infinitely many maximal torsion subvarieties and let Y_i be a complete list of them. For distinct i and j, $Y_i \cap Y_j$ is a proper torsion subvariety for both Y_i and Y_j (as both Y_i and Y_j are maximal torsion subvarieties of X). Moreover, because torsion subvarieties are irreducible by definition, we conclude

(46) $$\dim(Y_i \cap Y_j) < \min\{\dim(Y_i), \dim(Y_j)\}.$$

Hence, using (46) we obtain that for each k,

$$\left(\cup_{i=1}^{k-1} Y_i\right) \cap Y_k$$

is a proper torsion subvariety of Y_k. Because the torsion submodule ϕ_{tor}^N is Zariski dense in Y_k (see Corollary 4.14), we conclude that there exists a torsion point $x_k \in Y_k \setminus \left(\bigcup_{i=1}^{k-1} Y_i\right)$.

We will prove next that the sequence of torsion points $\{x_k\}$ is strict relative to Y. Let Z be a torsion subvariety of Y with $\dim(Z) < \dim(Y)$. We will show $X \cap Z$ contains finitely many x_k (note that by construction, $\{x_k\} \subset X$).

Because $\dim(Z) < M$, we can apply the induction hypothesis and conclude there are finitely many maximal torsion subvarieties of $X \cap Z$. Indeed, let $Z = \alpha + W$, where α is a torsion point and W is an irreducible algebraic ϕ-submodule. Then

(47) $$X \cap Z = \alpha + ((-\alpha + X) \cap W).$$

Thus we apply the inductive hypothesis to $X' := (-\alpha + X) \cap W$ and derive that $X' \subset W$ contains finitely many maximal torsion subvarieties. Therefore, $X \cap Z = \alpha + X'$ contains finitely many maximal torsion subvarieties. Let $W_1, \ldots, W_l \subset X \cap Z$ be a complete list of them. Because they are torsion subvarieties contained in X, for each $i \in \{1, \ldots, l\}$, there exists j such that $W_i \subset Y_j$. But each Y_j contains only finitely many x_k, by the construction of $\{x_k\}$. Hence, each of W_i contains only finitely many of the x_k and thus, Z contains finitely many of $\{x_k\}$ (we recall that $\{x_k\} \subset X$, by construction). This proves that the sequence $\{x_k\}$ is strict relative to Y.

Because $\dim(Y) = M$, there exists a suitable projection π of Y on M of the N coordinates of $\mathbb{G}_a^N$ such that π is a dominant morphism. At the expense of relabelling the coordinates of $\mathbb{G}_a^N$, we may assume $\pi : Y \to \mathbb{G}_a^M$. Moreover, because Y is an algebraic group, $\pi(Y)$ is also an algebraic group. Using $\dim(\pi(Y)) = M$ (because π is a dominant morphism), we conclude $\pi(Y) = \mathbb{G}_a^M$. Because $\dim(Y) = M = \dim(\pi(Y))$, we conclude each fiber of π is finite.

We claim the sequence $\{\pi(x_k)\} \subset \mathbb{G}_a^M(K^{\mathrm{sep}})$ is strict. Assume there exists some proper torsion subvariety $Z := \alpha + W \subset \mathbb{G}_a^M$ which contains infinitely many $\pi(x_k)$ (α is a torsion point and W is a proper algebraic ϕ-submodule of $\mathbb{G}_a^M$). Let S be the finite orbit of α under the action of ϕ on $\mathbb{G}_a^M$. Let $Z_0 := \cup_{\beta \in S} (\beta + W)$. Clearly, Z_0 is a proper algebraic ϕ-submodule of $\mathbb{G}_a^M$ $(\dim(Z_0) = \dim(W) < M)$. Moreover, by our assumption, Z_0 contains infinitely many $\pi(x_k)$.

Let $Z' := \pi^{-1}(Z_0) \subset Y$. Because Y is invariant under ϕ_t, then $\phi_t(Z') \subset Y$. Moreover,

$$\pi(\phi_t(Z')) = \phi_t(\pi(Z')) = \phi_t(Z_0) = Z_0.$$

Hence $\phi_t(Z') \subset Z'$. Using Lemma 4.11 we conclude Z' is a finite union of torsion subvarieties.

Because the kernel of π is finite, $\dim(Z') = \dim(Z_0) < M = \dim(Y)$. Moreover, because Z_0 contains infinitely many $\pi(x_k)$, Z' contains infinitely many x_k. Hence Z' is a finite union of torsion subvarieties of Y of dimension smaller than M, and Z' contains infinitely many x_k. This contradicts our proof that $\{x_k\}$ is strict relative to Y. We conclude $\{\pi(x_k)\}$ is a strict sequence of torsion points in $\mathbb{G}_a^M(K^{\mathrm{sep}})$.

Using Conjecture 4.4 for $g = M \leq N$ and for the strict sequence $\{\pi(x_k)\} \subset \phi_{\mathrm{tor}}^M$, we conclude $\overline{\delta}_{\pi(x_k)} \xrightarrow{w} \nu^{(M)}$. By the second reduction step for our proof of Theorem 4.15, X is invariant under $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. Thus $\pi(X)$ is invariant under $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. Hence the measures $\overline{\delta}_{\pi(x_k)}$ are all supported on $\pi(X(K^{\mathrm{sep}}))$. But $\pi(X(K^{\mathrm{sep}})) \subset \pi(X(K^{\mathrm{alg}}))$, which is a closed set in the v_∞-adic topology. Therefore, the weak limit $\nu^{(M)}$ is supported also on $\pi(X(K^{\mathrm{alg}}))$. But, by construction the support of $\nu^{(M)}$ is T^M, which contains the torsion submodule of $\mathbb{G}_a^M$. Therefore, $\pi(X)$ contains the torsion submodule of $\mathbb{G}_a^M$. As this torsion submodule is Zariski dense in $\mathbb{G}_a^M$ (see Corollary 4.13), we conclude $\pi(X) = \mathbb{G}_a^M$. Thus $\dim(X) = M = \dim(Y)$, which contradicts our first reduction step: $\dim(X) < M$. Therefore X has finitely many maximal torsion subvarieties. □

Theorem 4.6 for $g = N$ is an immediate corollary of Theorem 4.15.

Proof of Theorem 4.6. Assume X is not a torsion subvariety of $\mathbb{G}_a^N$. By Theorem 4.15 applied to $X \subset \mathbb{G}_a^N$, X is not the union Z of its maximal torsion subvarieties, because there are finitely many of them and each one has smaller dimension than X (here we use the irreduciblity of X). By construction, Z contains all the torsion points of X, which thus contradicts the hypothesis that the set of torsion points of $\mathbb{G}_a^N$ is dense in X. Therefore, X is indeed a torsion subvariety of $\mathbb{G}_a^N$. □

Assuming the validity of Conjecture 4.7 for all $g \leq N$, we prove the following generalization of Conjecture 4.9 for $g = N$.

Theorem 4.16. *Let Y be an algebraic ϕ-submodule of $\mathbb{G}_a^N$. Let X be a K^{sep}-subvariety of Y and let Z be the union of all (finitely many) maximal torsion subvarieties of X. If $Z \neq X$, then there exists a positive constant C (depending on X) such that for each $x \in (X \setminus Z)(K^{\mathrm{sep}})$, $\widehat{\mathrm{h}}(x) \geq C$.*

We first note that because we assumed the validity of Conjecture 4.7 for all $g \leq N$, we also assume the validity of Conjecture 4.4 for all $g \leq N$, because Conjecture 4.4 is a particular case of Conjecture 4.7. Hence Theorem 4.15 holds and we *do* know that X has finitely many maximal torsion subvarieties.

Before proving Theorem 4.16, we sketch the proof of Conjecture 4.9 using the result of Theorem 4.16 applied to $X \subset Y = \mathbb{G}_a^g$. If X is not a torsion subvariety, then it is not equal with the finite union Z of its maximal torsion subvarieties, because $\dim(Z) < \dim(X)$ (we also use here the fact that X is irreducible in Conjecture 4.9). Hence, there exists $C > 0$ as in Theorem 4.16. Let n be a positive integer such that $\frac{1}{n} < C$. Then X_n (defined as in Conjecture 4.9) is a subset of Z, which contradicts the hypothesis that X_n is dense in X. Therefore, our assumption was false and so, indeed X is a torsion subvariety.

Proof of Theorem 4.16. We proceed by induction on $\dim(Y)$. If $\dim(Y) = 0$, then both Y and X are finite unions of torsion points. Hence the theorem is vacuously true. We assume Theorem 4.16 holds for $\dim(Y) < M \leq N$ and we prove it also holds for $\dim(Y) = M$.

We may assume without loss of generality that $\dim(X) < M$. Otherwise, the irreducible components of X of dimension M are also irreducible components of Y and so, by Lemma 4.11, they are torsion subvarieties. Therefore, they are contained in Z. So, removing them will not change $X \setminus Z$.

At the expense of replacing Y and X by the respective finite unions of their orbits under the action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, we may assume that both Y and X are invariant under $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. Note that replacing X with $\cup_{\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)} \sigma(X)$, replaces $X \setminus Z$ with $\cup_{\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)} \sigma(X \setminus Z)$, which contains $X \setminus Z$.

Assume Theorem 4.16 does not hold for $X \subset Y$. Then we can find a sequence $\{x_k\} \subset (X \setminus Z)(K^{\mathrm{sep}})$ such that $\widehat{\mathrm{h}}(x_k) < \frac{1}{k}$ for each positive integer k. We prove next that the sequence $\{x_k\}$ is strict relative to Y.

Let Y' be a torsion subvariety of Y of dimension smaller than M and assume Y' contains infinitely many x_k. Let $Y' = \alpha + W$, where α is a torsion point and W is an (irreducible) algebraic ϕ-submodule of Y of dimension smaller than M. Then, as in (47),

$$X \cap Y' = \alpha + ((-\alpha + X) \cap W)$$

and so, we can apply the inductive hypothesis to $X \cap Y'$ (because $\dim(W) = \dim(Y') < M$). Note that the height function is not changed under translations by torsion points (this allows us to pass the inductive hypothesis from $(-\alpha + X) \cap Y'$ to $X \cap Y'$).

We conclude that either $X \cap Y'$ equals the finite union Z' of its maximal torsion subvarieties, or there exists a constant $C' > 0$ such that for every

$$x' \in ((X \cap Y') \setminus Z')(K^{\mathrm{sep}}),$$

$\widehat{\mathrm{h}}(x') \geq C'$. But the maximal torsion subvarieties of $X \cap Y'$ are contained in the maximal torsion subvarieties of X, which means that Z' contains no points from the sequence $\{x_k\} \subset (X \setminus Z)(K^{\mathrm{sep}})$. On the other hand, if $X \cap Y' \neq Z'$, then

$$\widehat{\mathrm{h}}(x_k) < \frac{1}{k} < C',$$

for every positive integer $k > \frac{1}{C'}$. So, there are finitely many points of the sequence $\{x_k\}$ contained in $((X \cap Y') \setminus Z')(K^{\mathrm{sep}})$. Therefore, Y' contains only finitely many points of the sequence $\{x_k\} \subset X$, which shows that indeed, $\{x_k\}$ is a strict sequence relative to Y.

We can redo now the argument from the last part of the proof of Theorem 4.15. Indeed, we find again a suitable projection $\pi : Y \to \mathbb{G}_a^M$ and prove as we did before, that $\{\pi(x_k)\}$ is a strict sequence (using that $\{x_k\}$ is a relative strict sequence). Because the height of a point in the affine space is the sum of the heights of each of its coordinates, $\widehat{\mathrm{h}}(\pi(x_k)) \leq \widehat{\mathrm{h}}(x_k)$, for each k. Hence $\lim_{k\to\infty} \widehat{\mathrm{h}}(\pi(x_k)) = 0$. Thus, we can apply the conclusion of Conjecture 4.7 for the strict sequence $\{\pi(x_k)\} \subset \mathbb{G}_a^M(K^{\mathrm{sep}})$ of small points and conclude that $\overline{\delta}_{\pi(x_k)} \xrightarrow{w} \nu^{(M)}$. This shows that the support T^M of $\nu^{(M)}$ is contained in $\pi(X(K^{\mathrm{alg}}))$. Hence $\pi(X) = \mathbb{G}_a^M$ and so, $\dim(X) = \dim(Y)$, contradicting our assumption that $\dim(X) < M$. Therefore there exists a uniform positive lower bound C for the height of the points in $(X \setminus Z)(K^{\mathrm{sep}})$. $\square$

References

[1] Y. Bilu, *Limit distribution of small points on algebraic tori.* Duke Math. J. 89 (1997), no. 3, 465-476.
[2] F. Breuer, R. Pink, *Monodromy groups associated to non-isotrivial Drinfeld modules in generic characteristic*, to appear in *The analogy between Number Fields and Function Fields*, Proceedings of the 4th Texel Conference, 2005.
[3] L. Denis, *Géométrie diophantienne sur les modules de Drinfeld.* (French) [Diophantine geometry on Drinfeld modules.] The arithmetic of function fields (Columbus, OH, 1991), 285-302, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.
[4] D. Ghioca, *The arithmetic of Drinfeld modules.* PhD thesis, University of California at Berkeley, 2005.
[5] D. Ghioca, *The Mordell-Lang Theorem for Drinfeld modules.* Internat. Math. Res. Notices, 2005, **53**, 3273-3307.
[6] D. Ghioca, *Points of small height on varieties defined over a function field.* submitted for publication, 2005.
[7] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 35. Springer-Verlag, Berlin, 1996.
[8] Thomas Scanlon, *Diophantine geometry of the torsion of a Drinfeld module.* J. Number Theory 97 (2002), no. 1, 10-25.
[9] E. Ullmo, *Positivité et discrétion des points algébriques des courbes.* (French) [Positivity and discreteness of algebraic points of curves] Ann. of Math. (2) 147 (1998), no. 1, 167-179.
[10] S. Zhang, *Equidistribution of small points on abelian varieties.* Ann. of Math. (2) 147 (1998), no. 1, 159-165.

Dragos Ghioca, Department of Mathematics & Statistics, Hamilton Hall, Room 218, McMaster University, 1280 Main Street West, Hamilton, Ontario L8S 4K1, Canada
E-mail address: dghioca@math.mcmaster.ca